FLIGHT SAFETY FOUNDATION
Airport Operations
Vol. 15 No. 3 *For Everyone Concerned with the Safety of Flight* May/June 1989

Controlling Employee Access

New FAA security regulations aim at closing the loophole of unauthorized access to airport operations areas.

by

Charles Spence

Safety for air travelers from hijackers, terrorists, or desperate persons has centered on limiting access through screening or authorized identification.

Mandatory security procedures at U.S. airports detected more than 40,000 firearms and caused about 18,000 related arrests since 1973. To some measure, this success of passenger screening, background checks, and ramp challenging brought about the newest change to the security rules. As control procedures improve, the criminal or terrorist seeks new ways to gain access to the air operations area (AOA) and other restricted locations, or to place destructive devices aboard aircraft.

One loophole in screening, which the U.S. Federal Aviation Administration (FAA) hopes to close with a recent amendment to Federal Aviation Regulation 107 is the use of expired, stolen or counterfeit identification badges (IDs) for airport, airline, and service companies.

An event in California prompted this. A disgruntled former airline employee flashed his company ID, bypassed the usual screening, and boarded an aircraft. En route to San Francisco he allegedly shot his former boss, who was a passenger on the flight, and the flight crew. The aircraft crashed, killing all 43 persons aboard.

James Burnley, then U.S. Secretary of Transportation, ordered the FAA to amend the security rules. An immediate step required flight crews to pass through the same screening as passengers, a procedure which has been objected to by some pilots. "We don't need guns to cause damage, destruction or deviation," the pilots pointed out. They cite their position of aircraft control throughout a flight. The FAA countered that it isn't just actual flight crews who need checking. Anyone can buy a uniform, steal or counterfeit an ID badge and enter an otherwise secure area.

A second action moved through the FAA in record time. Within a month after receiving instructions from Burnley, the FAA issued a Notice of Proposed Rule Making (NPRM). To emphasize the urgency, the agency allowed only 45 days for comment. This NPRM contained new requirements for control of access to airport secure areas. No longer would mere photo identification cards be enough to permit a person to enter a secure area. The proposed rule called for computer card access control or an alternative system that provided the same checks.

Aviation groups quickly attacked the proposal. Joint comments filed by five associations said the FAA underestimated the cost of card access security systems, failed to set uniform, compatible standards, and did not consider the limited number of suppliers to install systems in the allotted time. (The five U.S. associations were: Air-

port Operators Council International, Air Line Pilots Association, Air Transport Association of America, American Association of Airport Executives, and Regional Airline Association.)

Although unconfirmed, sources close to the FAA said the agency itself was not in favor of all the conditions of the regulation. Nor was the Office of Management and Budget. OMB reportedly was ready to return the rule to FAA without approval when the bombing of Pan Am flight 103 over Scotland occurred.

Faced with new pressures, FAA issued a final rule early in 1989, making minor changes from the original notice. Safety took precedence over price. Now, 270 airports in the United States must install tighter security procedures.

Since 1973, regulations have required limiting access to airport operations areas. However, the FAA says perimeter and near terminal access points have been weak links in airport security systems.

The new amendment, according to the FAA, merely strengthens existing regulations. Under this amendment, the security system must have four capabilities. It must:

- Ensure that only those persons authorized to have access to secured areas by the airport's security system are able to obtain that access;

- Ensure that such access is denied immediately at the access point, or points, to persons whose authority to have access changes;

- Provide a means to differentiate between persons authorized to have access to only a particular portion of the secured area and those authorized to have access to other portions or to the entire secured area; and,

- Be capable of limiting an individual's access by time and date.

For many, this is a difficult order.

In their comments seeking changes and time extensions in putting the rule into effect, the five associations pointed out that some airports have more than 1,800 access points.

Because the security systems would not necessarily be compatible, flight crew members complain they may be required to carry "a pocket full of different access cards," one for each airport into which they operate.

Some airport tenants see requirements of the amendment as virtually impossible to meet. As one general aviation facility operator at a Florida airport with commercial airline service puts it: "On a Sunday afternoon we may have as many as 100 general aviation airplanes all leaving at about the same time. With each having several passengers, there's no way we can escort all these people to their individual airplanes." Yet, the airport operator is charged with the responsibility of seeing that no unescorted or unbadged persons move into the airport operations area.

Unmoved by these concerns, however, the FAA set the following timetable:

- Each airport which screens more than 25 million persons annually must submit plans to the FAA by August 8, 1989 and have the system in place and operating within 18 months after approval by the FAA.

- Each airport which screens fewer than 25 million but at least two million persons annually, also must have plans to the FAA by August 8, 1989. They, however, will have 24 months after approval to get the system into operation.

- Other airports may take until February 8, 1990 for submission of plans. Installation and use of the system must be within 30 months after approval.

Originally, the FAA envisioned each airport would have a computer card access control system. While this still is expected for the larger airports, smaller facilities may install alternative systems provided they meet the four performance standards.

Quentin Johnson, manager of FAA's international aviation security branch, explains the standards. "Determining who has authorization to enter a secure area at a given time could be by personal recognition at points where pass-through is by only a few persons. As the list grows, other systems and methods must be employed." These can be lists generated by hand, personal computers, or minicomputers. The airport operator must be able to provide evidence that the system or procedure can distinguish between those who have authorized access from those who do not.

The system must be able to "immediately" deny access to someone who no longer has authorization to enter a particular area. The word "immediately" means within minutes for a person removed for a serious offense or who poses a safety risk to aviation, but may be longer for a person retiring or leaving under cordial conditions.

Control must be able to differentiate whether a person has authorization to have access to a particular secured area, to more than one, or to the entire secured area. An

employee of one airline, for instance, may have access to that company's particular secure area but would be prohibited from passing through secure areas of other carriers or through general airport access points.

Access must be controlled by time of day, work week, shift, or other time frame determined by the airport operator.

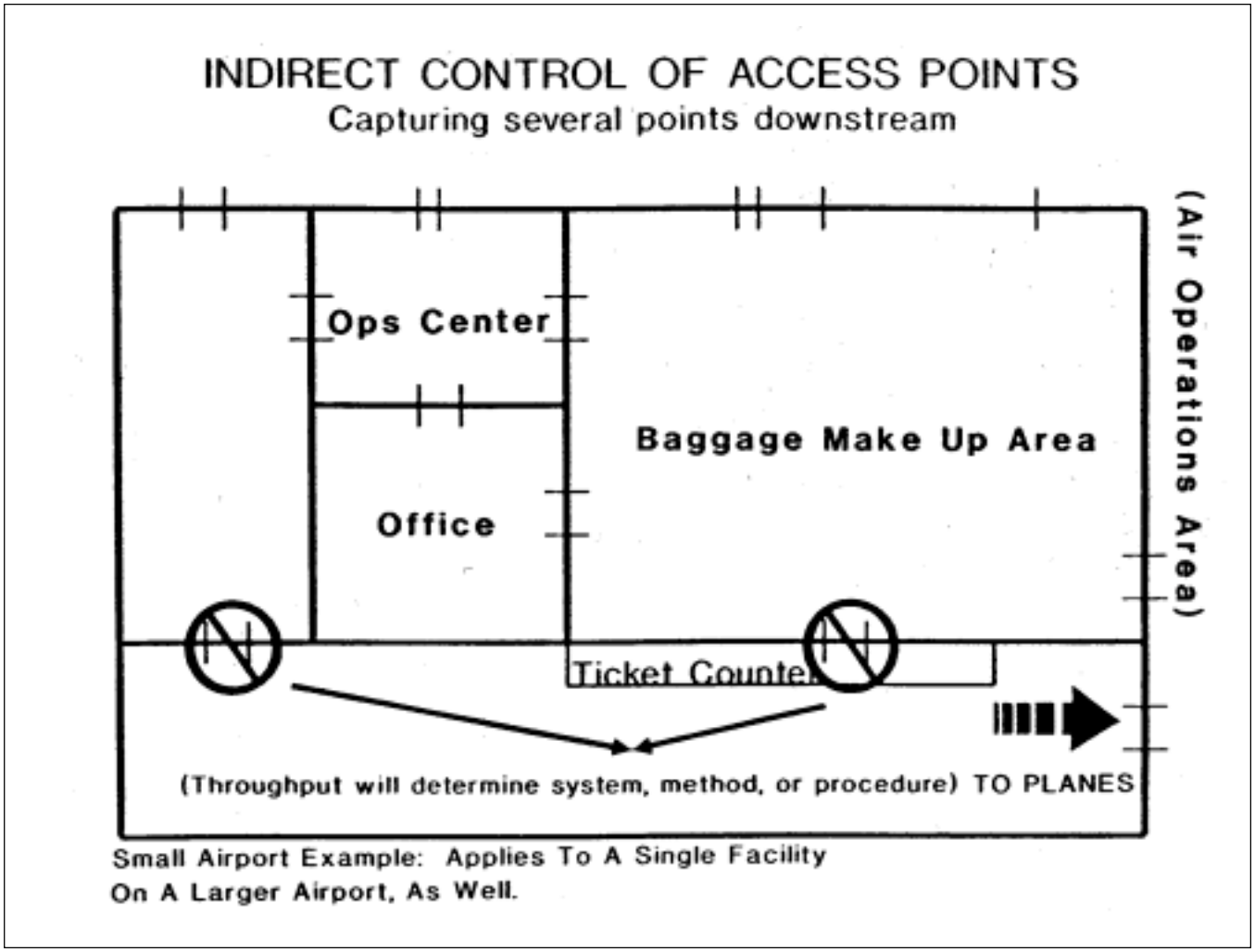
The airport authority has responsibility for securing the airport operations area and will face fines for violations which may occur. Tenants, however, can expect the requirements to be passed along to them. This applies particularly to general aviation fixed base operators, to cargo terminals, or other facilities in remote locations from terminal buildings where personnel screening has not been a common practice.

Transients, temporary workers and other persons not holding valid identification for the airport must be under escort. This, Johnson explains, has been a part of the regulations since 1973.

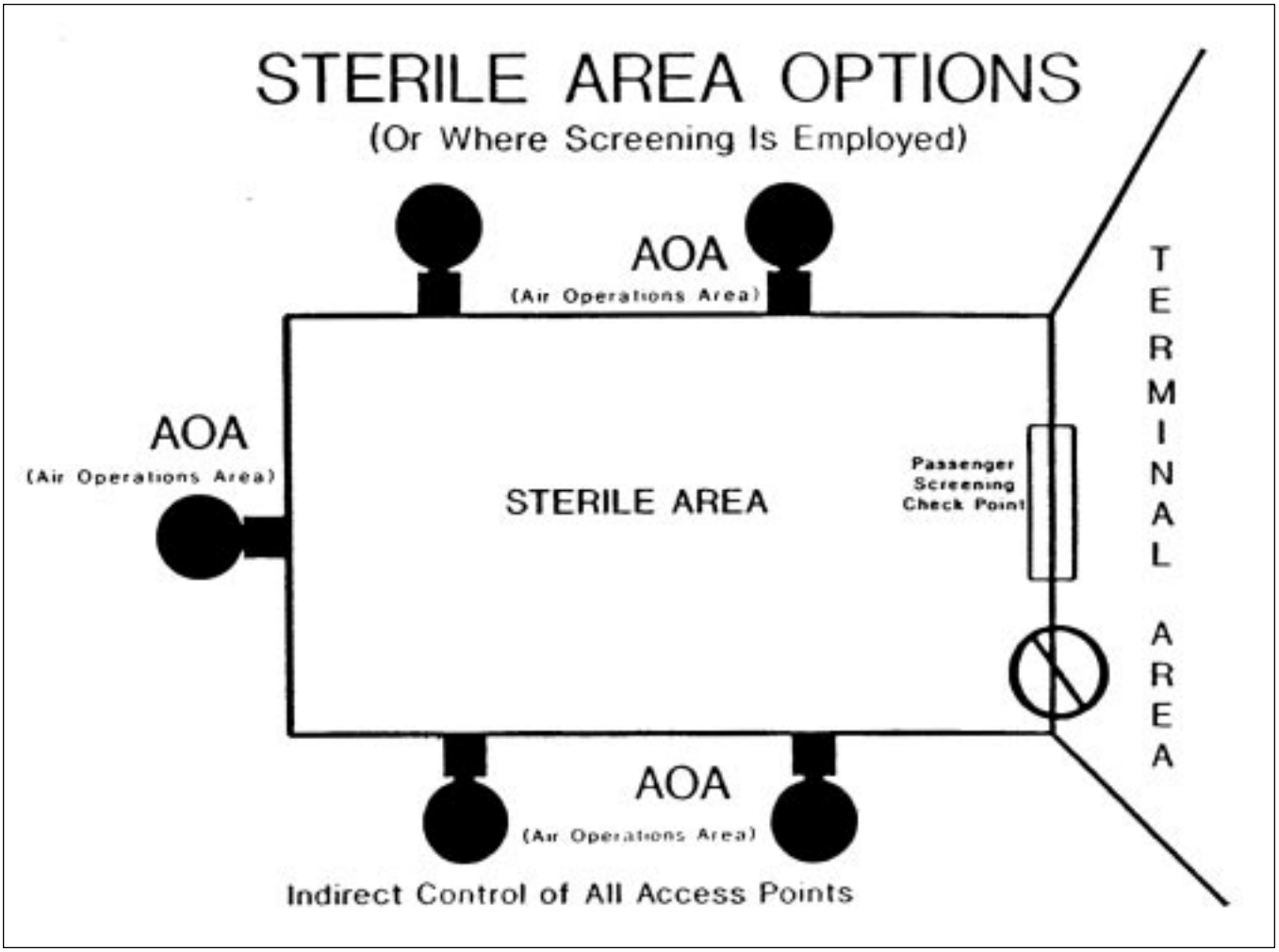
Designing and installing the control systems, according to the FAA, will not require additional efforts at the massive number of access points which concern airport operators. Johnson explains that several doors or gates may be controlled by directing card holders through a single access point into a sterile area while other doors remain secured. (See illustrations.)

Meeting the other requirements of the regulation may not be so easy, however. Take the example of an airline crew member who may have a dozen or 15 different coded access cards, one for each airport into which he or she flies. When that person's authority to enter secure areas changes — for discharge or other reasons — each airport will have to be notified and action taken to deny access. This must be "immediate" according to the FAA regulation.

Some groups, such as the Air Line Pilots Association, argue for a common system at each airport which would require access card. Such a common system is not unrea-



The FAA says two control points, such as this example for a small airport or for a single facility at a larger airport, serve as well as a control position at every access location.



Another indirect control example would place one control position to serve several access points. The employee entry position may be eliminated in this system if all employees pass through the approved passenger screening.

sonable, says Neal Owens, vice president of Sygnetron, a Timonium, Md., security firm. He says commonality can be achieved in the same way bank cards are prepared, which permits them to be used at different locations.

The president of another firm agrees. Lee Hargrave, Jr., of Casi-Rusco, says all that is needed is a hookup to have computers in various locations communicating with a common telephone line hookup.

Others disagree. Not only would the interconnecting lines be prohibitively expensive, they say, but a common system would defeat the purpose. Bob White, inside sales manager of National Control Systems, explains that a common system would give universal access to anyone who had a card.

Another argument against a common system points out that it would probably require a single supplier. This, opponents say, would delay installation and force airports to accept a system which may not be correct for every location. Nor does anyone foresee every airport agreeing on the same system and company for installation. The federal government would have to mandate a particular system, a move no one expects now.

Assuring safety through detection, apprehension, or diversion of threats continues to require change. Early hijackings involved mostly political refugees. C.J. Visser, a recognized authority on terrorism, reports that from 1947 to 1969, a period of 22 years, 113 hijackings of aircraft occurred (Flight Safety Foundation *Flight Safety Digest* - April 1988).

Most of these, he says, were conducted by persons seeking to use an aircraft for their own purposes. They wanted to escape from a political regime, return to a homeland, or embarrass their own states.

They set the pattern, Visser says, for others. In the next 18 years, more than 680 hijacks occurred; some for ransom money, others as terrorist tactics.

Since the initiation of airport security screening in 1973, more than nine billion persons have been screened in the U.S. and 9.9 billion pieces of carry-on luggage inspected. This dramatically reduced the number of hijackings. (FAA Semiannual Report to Congress on the Effectiveness of the Civil Aviation Security Program - June 1988).

In the five-year period before security screening, an average of 27 hijackings per year occurred. Mandatory screening reduced that number to an average of 7.2 per year.

Terrorists, to some degree thwarted by screening, continue to adapt new technologies. As lighter materials, such as fiber-reinforced composites and ceramics, replace metals in terrorist weapons, current detectors become less effective. Tiny, yet powerful, explosives are more easily hidden than are older types.

To meet these challenges, FAA is conducting an aggressive research and development program.

Two basic types of explosives detectors are now being developed under the FAA's program. One is a "sniffer" which can sense and identify the vapors from explosives. The other, using thermal neutron activation technology, produces electromagnetic energy or nuclear radiation. This energy or radiation interacts with the explosive, sensing and identifying the substance based on its composition.

Only the "sniffer" will be used to screen passengers. This has undergone on-site testing with encouraging results.

Encouraging also are results of the thermal neutron device. Initial airport testing took place at San Francisco International Airport. More than 20,000 pieces of checked baggage — a mixture of domestic and international — were examined. A computer made all decisions relating to the detection of explosive simulants within the luggage. No human decision-making or interpretation was involved in the detection process. Nationwide use of the thermal neutron device, FAA says, "could prevent explosives from getting on board aircraft in checked baggage or cargo."

Initial installations of the thermal neutron screening units are expected to occur this summer at a few key airports.

Thus, while computer card-controlled access becomes the newest action in maintaining security, it by no means will be the last. The FAA, law enforcement agencies, and airport operators continue to search for and adopt technologies and techniques to assure safety for the traveling public.♦

Identification Technologies

Many means are available to help airport management identify personnel who are authorized to have access to secure areas.

Technologies for positive identification range from magnetic bar codes to stored patterns of eye retinas. At least three dozen companies provide security services and products which could be used to comply with FAA regulations.

There are eight basic technologies in computerized security, according to Charles Sander, president of his own firm. Sander for 16 years was deputy chief of operations at Baltimore/Washington International Airport, considered by many to have one of the best card access control security programs.

Types one and two are **Mag Stripe**. Most credit cards use this technology. Data are magnetically encoded on the stripe much in the same way as a tape recording is made. One type of mag stripe card permits data to be erased and new data recorded. The other type cannot be erased by exposure to a magnetic field.

A third type is **Bar Code.** This method is commonly used for inventory control. It is found at many retail market check-outs. The computer reads the spaces between the bars. Another version of this is the infrared reader.

A fourth technology is known as **Finger Matrix.** In effect, this method stores a copy of the person's fingerprint on a card and in a computer and matches the two.

Bio Metrics, a fifth technology, scans the retina of a person's eye and stores these patterns in a computer. For identification, the computer matches the patterns

of the human eye with those stored.

A sixth technology is known as **Weigand Effect**. This uses a very thin wire that is heat tempered, stretched and twisted. It is then laminated into a card which, when run through a magnetic field, sends out a unique pulse pattern.

A seventh method is called **Bearium Ferrita**. Magnetic pellets are embedded on the edge of a laminated card. When the card is placed in a reader head, the pellets create a magnetic field that can be displayed as pulses. These pulses are converted to binary digits.

An eighth technology is the **Thin Film Chip**. This method laminates an integrated circuit into a card. The card "plugs in" to a reader. Through key strokes or audio, graphics can be produced, bringing up digitized photos, signatures, fingerprints or other means of personal identification.

Whatever the process, identification cards will be a continuing expense for an airport operator. Cards can cost as much as $7 each for some systems. With an airport averaging about a 30 percent annual turnover of persons authorized access, the price of security continues to increase.♦

42nd Annual International Air Safety Seminar

Hotel Athenaeum Inter-Continental

Athens, Greece

November 6-9, 1989

"The Human Element – Selection, Training and Development"

For more information contact Ed Peery, FSF

What's Your Input?

Flight Safety Foundation welcomes articles and papers for publication. If you have an article proposal, a completed manuscript or a technical paper that may be appropriate for *Airport Operations* please contact the Editor. Submitted materials are evaluated for suitability and a cash stipend is paid upon publication. Request a copy of "Editorial Guidelines for FSF Writers."

AIRPORT OPERATIONS

 • Subscriptions : $50 U.S. (U.S. - Canada - Mexico), $55 Air Mail (all other countries), six issues yearly. • Staff: Pat Dade, layout assistant; Jacque Edwards, word processor; Arthur H. Sanfelici, consultant • Request address changes by mail and include old and new addresses. • Roger Rozelle, editor, Flight Safety Foundation, 2200 Wilson Boulevard, Suite 500, Arlington, VA 22201-3306 U.S. • Telephone: 703-522-8300 • Telex: 901176 FSF INC AGTN • FAX: 703-525-6047